Notes for Algebraic Structures

Spring 2016

Transcribed by Jacob Van Buren
(`jvanbure@andrew.cmu.edu`)

Notes for Algebraic Structures, taught Spring 2016 at Carnegie Mellon University, by Professor Clinton Conley.

Administrativia

Instructor. Clinton Conley (`clintonc@andrew.cmu.edu`), WEH 7121
`http://www.math.cmu.edu/~clintonc/`

Grading. 20% HW, 20% $\times$ 2 midterms, 40% Final

Homework. Wednesday-Wednesday. Graded for completeness, one starred problem for which no collaboration of any type is allowed.
Most homework out of textbook ("D&F").

Contents

The Integers

Lecture 1 (2016–01–11)

Notation. $\mathbb{N} := \{1, 2, 3, \ldots\}$ in this class.

Properties: Order, other things. Least element in a set S: $x \in S$ s.t. $\forall y \in S, x \leq y$
Addition $(\mathbb{Z}, +)$:

- Associativity $(x + y) + z = x + (y + z)$
- Identity $x + 0 = 0 + x = 0$
- Inversion $x + (-x) = (-x) + x = 0$
- Commutativity $x + y = y + x$

Multiplication $(\mathbb{Z}, +, \cdot)$:

- Associative
- Distributive
- Identity ("1")

Integer division: Assume x an integer and $y \in \mathbb{Z}^+$ then $\exists! d \in \mathbb{Z}, \exists! r \in \mathbb{Z} : 0 \leq r < y, x = d \cdot y + r$

Definition 1. $y|x$ "y divides x" iff $\exists d \in \mathbb{Z} : x = d \cdot y$.

E.g. $3|9, 4 \not| 7$.

Definition 2. d is a GCD of x and y if

- $d|x, d|y$
- If $c|x$ and $c|y$ then $c|d$

Lecture 2 (2016–01–13)

Definition 3. Given $a, b \in \mathbb{Z}$, denote by $\mathbb{Z}(a, b)$ the set $\{ax + by | x, y \in \mathbb{Z}\}$.

Theorem 4 (Euclid, Bezout). *Suppose $a, b \in \mathbb{Z}$ are nonzero and let d be the smallest positive element of $\mathbb{Z}(a, b)$, then d is the unique positive GCD of a and b.*

Proof. d is a GCD of a, b

(1) (Existence of positive GCD)
  (a) By integer division, $\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$. If $r = 0$ then $d|a$, so done. Otherwise, suppose $0 < r < d$, so $r = a - qd$ since $d \in \mathbb{Z}(a, b)$, we may fix x, y st $d = ax + by$, meaning $r = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in \mathbb{Z}(a, b)$, meaning d was not the minimal positive element in $\mathbb{Z}(a, b)$, RAA. Thus, $d|a$
  (b) Homework: If $c|a$ and $c|b$ then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$ Hence $c|d$

(2) (Uniqueness of positive GCD) Suppose d_1, d_2 are both positive GCDs of a and b. $d_1|d_2$ and $d_2|d_1$ as they are both GCDs. i.e., $\exists m, n \in \mathbb{Z}$ such that $d_2 = md_1$ and $d_1 = nd_2$. As $\text{sgn}(d_1) = \text{sgn}(d_2)$, $m \geq 0$ and $n \geq 0$. As $d_1 = mnd_1$, $m = n = 1$. Thus $d_1 = d_2$.

□

Definition 5. <u>Relatively prime</u> $\iff$ $\gcd(a, b) = 1$

Theorem 6. *If p is prime, $a, b \in \mathbb{Z}$ are nonzero, and $p|(ab)$, then $p|a$ or $p|b$.*

Proof. Consider $d = \gcd(p, a)$. Since $d|p$, we know $d = p$ or $d = 1$.

If $d = p$: By def of GCD, $d|p$ and $d|a$ i.e. $p|p$ and $p|a$ so we're done.

If $d = 1$: Fix integers x and y such that $px + ay = 1$. $b = p(xb) + (ab)y$ as $p|p(xb)$ and $p|\underbrace{(ab)}_{\uparrow}y$, $p|b$.

□

Theorem 7 (Unique Prime Factorization). *Suppose that $a > 1$ an integer, $m, n \geq 1$ and $p_1 \leq p_2 \leq \ldots \leq p_m, q_1 \leq q_2 \leq \ldots \leq q_m$ are positive primes.*

Then $m = n$ and $p_i = q_i$ for all i.

Proof. By induction, it suffices to show $p_1 = q_1$. Suppose not. WLOG, assume $p_1 < q_1$. We know that $p_1|a$ (as $p_1|q_1q_2 \ldots q_n$) Hence, $\exists i \leq n$ such that $p_i|q_i$. since p_i and q_i prime, $p_1 = q_i$. However, $p_1 < q_1 \leq q_i = p_1$ so $p_1 < p_2$ contradiction.
Hence $p_1 = q_1$ so by induction, we're done. □

Lecture 3 (2016–01–15)

Teaser: Construct numbers of the form $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.
Notion of addition still exists: (similar to complex numbers, coefficients remain integers)
Same with multiplication
Among these "numbers", 2 is irreducible. But, 2 is not prime, as $2 \not| (1 + \sqrt{-5})$ and $2 \not| (1 + \sqrt{-5})$, but $2 | \underbrace{(1 + \sqrt{-5})(1 - \sqrt{-5})}_{=6=2\cdot 3}$.

The Integers (mod n)

For today, $n > 0$.

DEFINITION 8. For $a, b \in \mathbb{Z}$ we say $a \equiv b \pmod{n}$ iff $n \,|\, (b-a)$.

$\equiv$ is an *equivalence relation*

- Reflexivity: $a \equiv a$
- Symmetry: $a \equiv b \iff b \equiv a$
- Transitivity: $a \equiv b \wedge b \equiv c \implies a \equiv c$

PROOF. We know that $a \equiv b$ and $b \equiv c$, i.e. $n \,|\, (b-a)$ and $n \,|\, (c-b)$ We want $a \equiv c$, i.e., $n \,|\, (c-a)$

$$c - a = c + (-b + b) - a = \underbrace{(c-b) + (b-a)}_{n \text{ divides these}}$$

$\square$

DEFINITION 9. Denote by $\overline{a}$ or $[a]_n$ the <u>equivalence class</u> of a with respect to $\equiv \pmod{n}$ (I.e., The set $\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \overline{\{a + kn : k \in \mathbb{Z}\}}$).

EXAMPLE. If $n = 2$, there are 2 equivalence classes:
$\overline{0} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \overline{2} = \overline{-36}$
$\overline{1} = \{\ldots, -3, -1, 1, 3, \ldots\}$

DEFINITION 10. Denote by $\mathbb{Z}/n\mathbb{Z}$ the collection of all $\equiv \pmod{n}$ equivalence classes.

E.g. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
"Define" addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Makes sense, but we need to check that this definition makes any sense at all (make sure it's *well-defined*). Specifically, we need to make sure that the results of these operations doesn't depend on the representatives of the equivalence classes we chose (e.g. check that $\overline{x} + \overline{z} \equiv \overline{y} + \overline{z}$ if $x \equiv y$).
For brevity, we just show addition.

THEOREM 11. $+$ *and* $\cdot$ *are well-defined on* $\mathbb{Z}/n\mathbb{Z}$

PROOF. (of $\cdot$) Assume that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then, we want to show that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
We know: $n \,|\, (a_2 - a_1)$ and $n \,|\, (b_2 - b_1)$.

We want: $n \,|\, (a_2b_2 - a_1b_1)$.

$$\begin{aligned} a_2b_2 - a_1b_1 &= a_2b_2 + (-a_1b_2 + a_1b_2) - a_1b_1 \\ &= (a_2b_2 - a_1b_2) + (a_1b_2 - a_1b_1) \\ &= \underbrace{(a_2 - a_1)b_2 + a_1(b_2 - b_1)}_{n \text{ divides these}} \end{aligned}$$

So, $n \,|\, (a_2b_2 - a_1b_1)$ as desired $\square$

Remark: This is a special case of a "quotient construction," in which you start with a set and an equivalence relation on it and operations on the set that "respect" the equivalence relations (i.e. equivalent inputs yield equivalent outputs)
More notes: Multiplicative inverses are uncommon in the integers (only for 1 and -1). However, it's "more prevalent" in $\mathbb{Z}/n\mathbb{Z}$ in the following sense:

THEOREM 12. *Suppose $n > 0$ is an integer, $a \in \mathbb{Z}$ such that $\gcd(n, a) = 1$ (they're coprime). Then there is $b \in \mathbb{Z}$ such that $ab = 1 \pmod{n}$ (alternatively, $\overline{a} \cdot \overline{b} = \overline{1}$)*

PROOF. Use Bézout's identity (from last lecture) Take integers x, y such that $nx + ay = \gcd(a, n) = 1$. Then, $nx = 1 - ay$, so $n \,|\, (1 - ay)$, so $1 \equiv ay \pmod{n}$, Choose $b = y$ and we're done ($\overline{a}\overline{b} \equiv \overline{1}$). $\square$

Groups

Definition 13. We say that $*$ is a binary operation on some set X if it is a function $* : X \times X \to X$. (That is, $*$ accepts two (ordered) inputs from X and it outputs one element of X.)

Remark: usually write $a * b$ for the output of $*$ on the input (a, b).

Definition 14. A group is a set G with a binary operation $*$ (often abbreviated $(G, *)$) satisfying the following 3 axioms.

i. Associativity: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$
ii. Identity: There is some $e \in G$ such that $\forall a \in G : a * e = e * a = a$
iii. Inversion: $\forall a \in G(\exists b \in G(a * b = b * a = e))$ (where e is as described in ii)

Lecture 4 (2016–01–20)

Recall the definition of a group.

Definition 15. $(G, *)$ is an abelian (commutative) group if it is a group and

iv. $(G, *)$ is commutative $(\forall x, y \in G : x * y = y * x)$

Let $(G, *)$ be an arbitrary but fixed group.

Proposition 16. *There is a unique identity element.*

Proof. Suppose e and f both satisfy the second group property. we compute $e * f$ in two ways. $e * f = f$ and $e * f = e$, so by transitivity, $e = f$. $\square$

Proposition 17. *If $a \in G$, a has a unique inverse.*

Proof. Suppose that b and c are both inverses for a, $b * a = e$, $a * c = e$. Then,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

$\square$

Notational Conventions.

- We will often just call a group G instead of $(G, *)$
- We abbreviate multiplication $(x * y)$ as $x \cdot y$ or just xy
- We will often write xyz for $(x * y) * z$ (due to associativity)
- When working with $(\mathbb{Z}, +)$, we'll just use $+$
- We'll denote the (unique) identity of G by 1 or by e.
- We'll denote the inverse of x by x^{-1}
- Given an integer exponent $n \in \mathbb{Z}$ and $x \in G$, define

$$x^n = \begin{cases} \prod_{i=1}^{n} x, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ \prod_{i=1}^{-n} (x^{-1}), & \text{if } n < 0 \end{cases}$$

Group Examples. "Definition:" $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^+ \right\}$

(1) $(\mathbb{Z}, +)$ is an abelian group
(2) $(\mathbb{Z}, \times)$ is not a group
    Why? 2 has no inverse in $\mathbb{Z}$. $(\nexists x \in \mathbb{Z} : (2x = 1))$
(3) $(\mathbb{Q}, +)$ is an abelian group
(4) $(\mathbb{Q}, \times)$ is not a group (0 has no inverse)
(5) $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group.
(6) $\mathrm{GL}(n)$ is the set of matrices $A_{n\times n}$ for which $\det A_{n\times n} \neq 0$
(7) The set G of 2×2 matrices with determinant 1, along with matrix multiplication, is a group. Called the "special linear group."

Closure:

$$\det\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)\right) = (bc - ad)(fg - eh) = 1$$

i. Associativity: proof left for the reader.
ii. Identity: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
iii. Given $a = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, take $a^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, which you can verify is still in G.

The group is *not* abelian. Take $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Verify that $ab \neq ba$

(8) Suppose that $X \neq \emptyset$ is some set, and denote by S_X the set of bijections $f : X \to X$. Then $(S_X, \circ)$ is a group, where $\circ$ is function composition. ($(f \circ g)$ is the function $x \mapsto f(g(x))$.)
    Identity is $x \mapsto x$. Inversion $f^{-1} = f^{-1}$.

Symmetric Groups

Lecture 5 (2016–01–25)

Recall: if X is a set then S_X is the group of bijections on it.

DEFINITION 18. S_X (or Sym_X) is called the symmetric group on X.

Note: $\circ$ is associative because $(f \circ g) \circ h$ is

$$x \overset{\mathsf{h}}{\mapsto} (x) \overset{\mathsf{g}}{\mapsto} g(h(x)) \overset{\mathsf{f}}{\mapsto} f(g(h(x)))$$

Note: if $X = \{1, \ldots, n\}$, then we usually write $\underline{S_n}$ instead of $S_{\{1,\ldots,n\}}$. (Sometimes called symmetric group of degree n.)

Let's examine S_3:

elt.	1	2	3
e	1	2	3
a	1	3	2
b	2	1	3
c	2	3	1
d	3	1	2
f	3	2	1

The group has $6 = 3!$ elements.
Lets compute ab and ba
$ab = a \circ b$, looking it up in the table gives $ab = d$ and $ba = c$.
In particular, S_3 is not abelian.

DEFINITION 19. A cycle is a permutation σ of the following form:

There is a sequence $x_1, x_2, \ldots, x_m$ of finitely many (distinct) elements of $\{1, 2, \ldots, n\}$ such that $\sigma(x_{i-1}) = x_i$, $\sigma(x_m) = x_1$, and $\sigma(y) = y$, for $y \notin \{x_1, \ldots, x_m\}$.
We call m the length of the cycle.

Ex. In S_3, $d = \frac{1\,2\,3}{3\,1\,2}$ is a cycle of length 3, with $x_1 = 1, x_2 = 3, x_3 = 2$.

Ex. In S_3, $a = \frac{1\,2\,3}{1\,3\,2}$ is a cycle of length 2, with $x_1 = 2, x_2 = 3$.

NOTATION. Given a cycle, we can efficiently denote it by $(x_1\, x_2\, x_3\, \ldots\, x_m)$.

EXAMPLE. In S_3, $a = \frac{1\,2\,3}{1\,3\,2}$ would be written as (1 3 2).

Let's work in S_5.
$\varphi := \frac{1\,2\,3\,4\,5}{3\,4\,1\,5\,2}$ is not a cycle, but it is the "superposition" of two cycles (1 3) and (2 4 5). Thus, we may write $\varphi =$(1 3) $\circ$ (2 4 5), or (2 4 5)(1 3).

THEOREM 20. *Every permutation in S_n may be written as the product of "disjoint" cycles. (The identity is the empty product).*

PROOF. Sketch: If you have e then you're done trivially.
Otherwise, fix the least element x of $\{1, \dots, n\}$ "moved" by σ (i.e. $\sigma(x) \neq x$). Look at $x, \sigma(x), \sigma^2(x), \dots, \sigma^m(x) = \sigma^n(x)$, $n < m$. So, as σ is invertible, $\sigma^{m-n}(x) = x$, so x is part of a cycle. $\square$

THEOREM 21. *Cycles can be written as a product of transpositions.*

General propositions on inversion in groups. Let G be a group, and let $a, b, x \in G$ be arbitrary.

- $(a^{-1})^{-1} = a$

  PROOF. Show that a is the inverse of a^{-1}. Follows from group axiom. $\square$

- $(ab)^1 = b^{-1}a^{-1}$

  PROOF. $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Similarly, this works when we multiply from the other side. $\square$

Lecture 6 (2016–01–27)

DEFINITION 22. The cardinality (or order) of a group G is the number of elements in it, denoted by $|G|$.

EXAMPLE.

- $|\mathbb{Z}| = \infty (= \aleph_0)$
- $|(\mathbb{Z}/5\mathbb{Z})| = 5$
- $|S_4| = 4! = 24$

DEFINITION 23. Given a group G and $x \in G$, the order of x is the smallest integer $n > 0$ such that $x^n = e$. If no such n exists, we say the order is ∞.
We denote by $|x|$ the order of x.

EXAMPLE. In $(\mathbb{Z}, +)$: $|0| = 1$, $|5| = \infty$.
In S_5: $|(1\ 3)| = 2$, $|(2\ 4\ 5)| = 3$, $|(1\ 3)(2\ 4\ 5)| = 6$.

PROPOSITION 24. *If G is a* finite *group, every $x \in G$ has finite order. Moreover, $|x| \leq |G|$.*

PROOF. Say $|G| = k$. Consider the sequence $x^0, x^1, x^2, \dots, x^k$. There are $k + 1$ items in the sequence. So $\exists m < n$ such that $x^m = x^n$. $x^{n-m} = x^n x^{-m} = x^m x^{-m} = e$. As $0 < n - m \leq k$, it follows that $|x| \leq n - m \leq |G|$. $\square$

Subgroups

Definition 25. Suppose $(G, *)$ is a group and $H \subseteq G$ some subset of G. We say H is a <u>subgroup</u> of G, written $H \leq G$ if $(H, *)$ happens to be a group, i.e., the following properties hold:

$*$ is a associative binary operator on H (i.e., it's closed) with inverses and an identity element.

Example.

- $\mathbb{Z} \leq \mathbb{Q}$ (under addition)
- Even integers $\leq \mathbb{Z}$ (under addition)
- $n\mathbb{Z} \leq \mathbb{Z}$, where $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$
  Aside: every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$
- $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$.

Proposition 26. *(Homework): $H \leq G$ iff*
(a) $H \neq \emptyset$ (nonempty)
(b) $\forall x, y \in H(xy \in H)$ (closed under product)
(c) $\forall x \in H(x^{-1} \in H)$ (closed under inverses)

Proposition 27. *Suppose G is a* finite *group. Then $H \leq G$ iff $H \neq \emptyset$ and $\forall x, y \in H$: $xy \in H$.*

Proof. We show that for $H \subseteq G$ (a) and (b) $\implies$ (c) (letters from proposition (26))
Fix $x \in H$. Since G is finite, $|x|$ is finite (in G). Say $|x| = n > 0$ $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} = e_G$.

Hence, $e_G \in H$.
Examine x^{n-1}.

$$x^{n-1} = \begin{cases} x^0 = e & \text{if } n = 1 \\ \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} & \text{if } n > 1 \end{cases}$$

But $x^{n-1} = x^{-1}$, since $x^{n-1}x = x^n = xx^{n-1} = e$. Thus, (c) holds for H. $\square$

Remark. $\mathbb{N} = \{0, 1, \ldots\} \subseteq \mathbb{Z}$, but $\mathbb{N} \not\leq \mathbb{Z}$, despite satisfying (a) and (b).

(Left) Coset equivalence

Suppose G is a group and $H \leq G$ is a subgroup of G.

DEFINITION 28. We say $x \sim y \pmod{H}$ if $x^{-1}y \in H$.

PROPOSITION 29. $\sim \pmod{H}$ *is an equivalence relation.*

PROOF.

- Reflexivity $(x \sim x)$:
  $x^{-1}x = e \in H$, so $x \sim x$.
- Symmetry $(x \sim y \implies y \sim x)$:
  We know $x^{-1}y \in H$. H is closed under inversion, so $H \ni (x^{-1}y)^{-1} = (y^{-1}(x^{-1})^{-1}) = (y^{-1}x)$. Thus, $y \sim x$.
- Transitivity $((x \sim y) \wedge (y \sim z) \implies (x \sim z))$:
  We know $x^{-1}y \in H$ and $y^{-1}z \in H$.
  Thus, $H \ni (x^{-1}y)(y^{-1}z) = x^{-1}ez = x^{-1}z$, so $x \sim z$.

□

Lecture 7 (2016–01–29)

G is a group. $H \leq G$ a fixed subgroup of G.
Given $x, y \in G$, $x \sim y \pmod{H}$ iff

$$x^{-1}y \in H.$$

Last time: we showed it was an equivalence relation.
What are the equivalence classes of $\sim \pmod{H}$? We examine

$$\begin{aligned}
[x] &= \{y \in G : x \sim y \pmod{H}\} \\
&= \{y \in G : x^{-1}y \in H\} \\
&= \{y \in G : \exists h \in H(x^{-1}y = h)\} \\
&= \{y \in G : \exists h \in H(x(x^{-1}y) = xh)\} \\
&= \{y \in G : \exists h \in H(y = xh)\}
\end{aligned}$$

So, $[x]$ is exactly the set

$$\{xh : h \in H\}.$$

NOTATION. We write xH to abbreviate the set $\{xh : h \in H\}$.

DEFINITION 30. The equivalence class xH is called the (left) <u>coset</u> of x with respect to H.

NOTATION. The cyclic subgroup of x is denoted by $\langle x \rangle$.

Examples:

- $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$ = multiples of n. So $H \leq G$. For $x \in \mathbb{Z}$, its coset is $\overline{x} = \{x + h : h \in n\mathbb{Z}\} = \{x + nk : k \in \mathbb{Z}\}$
- $G = S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ Take $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3$ (the cyclic subgroup of $(1\ 2\ 3)$).

  So what are the cosets? $eH = \{eh : h \in H\} = \{h : h \in H\} = H$. (In general, eH is always just H). (Even more generally, $xH = H$ whenever $x \in H$.)

  Another coset is $(1\ 2)H$. Just compute $(1\ 2)h$ for each $h \in H$. Thus

$$(1\ 2)H = \left\{ \begin{array}{lll} (1\ 2) & e & = (1\ 2) \\ (1\ 2) & (1\ 2\ 3) & = (2\ 3) \\ (1\ 2) & (1\ 3\ 2) & = (1\ 3) \end{array} \right\} = \{(1\ 2), (2\ 3), (1\ 3)\}$$

  We note that $(1\ 2)H = (2\ 3)H = (1\ 3)H$, as each of those are in $(1\ 2)H$.
- $G = S_3$, $K = \langle (1\ 3) \rangle = \{e, (1\ 3)\} \leq G$. Analyze cosets mod K.

  Easy coset: $eK = K$.

  For the next coset, choose $(1\ 2\ 3)K$

$$(1\ 2\ 3)K = \left\{ \begin{array}{ll} (1\ 2\ 3)\ e & = (1\ 2\ 3) \\ (1\ 2\ 3)\ (1\ 3) & = (2\ 3) \end{array} \right\} = \{(1\ 2\ 3), (2\ 3)\}$$

  Next coset after that is $(1\ 2)K = \{(1\ 2), (1\ 3\ 2)\}$.

  We note that the equivalence classes mod K partition S_3, Although they are not all subgroups.

In the last two examples, it wasn't a coincidence that each coset was of the same cardinality.

PROPOSITION 31. *Suppose G is a group, $H \leq G$, and $x \in G$. Then $|xH| = |H|$.*

PROOF. We establish a bijection between H and xH.
Define $\varphi : H \to xH$, $\varphi(h) = xh$.

CLAIM (1). φ is surjective.

PROOF. Suppose $y \in xH$.
By definition of xH, $\exists h \in H$ such that $y = xh$. So, $y = \varphi(h)$. □(C1)

CLAIM (2). φ is injective.

PROOF. Suppose $h_1, h_2 \in H$ such that $\varphi(h_1) = \varphi(h_2)$.
By definition of φ, we have $xh_1 = xh_2$. Since G is a group, x has an inverse x^{-1}.
Thus, $x^{-1}(xh_1) = x^{-1}(xh_2) \implies h_1 = h_2$ as desired. □(C2)

Thus φ is a bijection, meaning $|xH| = |H|$ as desired. □(Prop.)

THEOREM 32 (Lagrange's Theorem). *Suppose that G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

PROOF. Left coset equivalence partitions G into k equivalence classes of size $|H|$.
Thus $|G| = k|H|$, as desired. □

COROLLARY 33. *Suppose that G is a finite group and $x \in G$. Then $|x|$ divides $|G|$.*

PROOF. Consider $\langle x \rangle$ (the cyclic subgroup generated by x). $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$, where $|x| = n$. $|\langle x \rangle| = n$. Hence $n = |x|$ divides $|G|$. □

Lecture 8 (2016–02–01)

We go to the previous lecture for examples.
Consider $G = S_3, H = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq G$, $K = \langle(1\ 3)\rangle = \{e, (1\ 3)\} \leq G$.

Definition 34. If G is a group and $H \leq G$, denote by G/H (G "mod" H) the collection of (left) cosets of H in G.

Example.
(a) $n\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
(b) $S_3/H = \{eH, (1\ 2)H\}, \quad eH = H, \quad (1\ 2)H = \{(1\ 2), (2\ 3), (1\ 3)\}$
(c) $S_3/K = \{\{e, (1\ 3)\}, \{(1\ 2\ 3), 23\}, \{(1\ 2), (1\ 3\ 2)\}\}$

Normal Subgroups

Fundamental question: When is there "natural" group operation on G/H? Prototype: $\mathbb{Z}/n\mathbb{Z}$, $\overline{x} + \overline{y} = \overline{x+y}$.
Natural Attempt:

$$(g_1H)(g_2(H)) \stackrel{?}{=} (g_1g_2)H.$$

This works fine for (b) in the sense that if $g_1H = g_2H$ and $k_1H = k_2H$ then $(g_1k_1)H = (g_2k_2)H$ (verification left to reader).
But it *doesn't* work for (c). e and $(1\ 3)$ both represent eK. But they give *different* cosets after multiplication by $(1\ 2\ 3)$.

- $e(1\ 2\ 3) = (1\ 2\ 3)$
- $(1\ 3)(1\ 2\ 3) = (1\ 2)$.

In general, what would we need to have, in order to have multiplication in G/H be "well-defined?"
We want: $\underbrace{x_1 \sim x_2}_{x_1^{-1}x_2 = h \in H}$ and $\underbrace{y_1 \sim y_2}_{y_1^{-1}y_2 = k \in H} \implies x_1y_1 \sim x_2y_2$. Thus, we want $(x_1y_1)^{-1}(x_2y_2) \in H$.

$$(x_1y_1)^{-1}(x_2y_2) = (y_1^{-1}x_1^{-1})(x_2y_2) = y_1^{-1}(x_1^{-1}x_2)y_1k = \underbrace{y_1^{-1}hy_1}_{\in H}\underbrace{k}_{\in H} \in H$$

This expression motivates the definition of a <u>normal subgroup</u>

Definition 35. If G is a group, and $N \leq G$, we say N is <u>normal</u> if for all $n \in N$, and $g \in G$, we have $g^{-1}ng \in N$. We write this as $N \trianglelefteq G$.

Remark. For fixed $g \in G$, the map for $x \in G$

$$x \mapsto g^{-1}xg$$

is called <u>conjugation by g</u>.

Thus, N is normal if it is stable under all conjugation.

Theorem 36. *Let G a group $H \leq G$. Then the following are equivalent:*
(I) $(g_1H)(g_2H) = (g_1g_2)H$ is a well-defined group operation on G/H.
(II) $H \trianglelefteq G$.

(II) $\implies$ (I). $x_1^{-1}x_2 = h, y_1^{-1}y_2 = k$. (Exercise for the reader) ∎

(I) $\implies$ (II). Suppose $h \in H$ and $g \in H$ want $g^{-1}hg \in H$.
Note: $e \sim h$ since $e^{-1}h = h \in H$.
By (I),we have $(eg)H = (eH)(gH) = (hH)(gH) = (hg)H$.
So, $gH = (hg)H$, meaning $g \sim hg$, so $g^{-1}hg \in H$. $\square$(Thm)

PROPOSITION 37. *If G is abelian, every subgroup is normal.*

PROOF. Fix $H \leq G$, $h \in H$, $g \in G$. Then $g^{-1}hg = g^{-1}gh = h \in H$. $\square$

PROPOSITION 38. $G \trianglelefteq G$ *and* $\{e\} \trianglelefteq G$.

PROOF. $g^{-1}hg \in G$ and $g^{-1}eg = g^{-1}g = e \in \{e\}$. $\square$

DEFINITION 39. For $A \subseteq G$, denote by $g^{-1}Ag$ the set $\{g^{-1}ag : a \in A\}$.
Called <u>the conjugate of A by G</u>.

REMARK. Thus, N is normal iff $N \leq G$ and $\forall g \in G : g^{-1}Ng \subseteq N$.

PROPOSITION 40. $N \trianglelefteq G \implies \forall g \in G : g^{-1}Ng = N$

PROOF. Fix $n \in N$. we want $n \in g^{-1}Ng$. (This shows $N \subseteq g^{-1}Ng$.)
We know by $N \trianglelefteq G$ that $m = (g^{-1})^{-1}n(g^{-1}) \in N$. Then $m = gng^{-1}$.

CLAIM. $g^{-1}mg = n$

PROOF. $g^{-1}(gng^{-1})g = \cancel{(g^{-1}g)}n\cancel{(g^{-1}g)} = n$ $\square$(Claim)

$\square$(Prop)

Homomorphisms

DEFINITION 41. Suppose G, H are groups and $\varphi : G \to H$ is a function. We say φ is a homomorphism if $\forall g_1, g_2 \in G : \phi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$.

DEFINITION 42. Suppose $\varphi : G \to H$ is a homomorphism. The Kernel of ϕ is $\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\})$.

PROPOSITION 43. *Suppose $\varphi : G \to H$ is a homomorphism between groups.*
Then $K = \mathrm{Ker}(\varphi) \trianglelefteq G$.

PROOF.

CLAIM (1). $K \neq \emptyset$. In fact, $e_G \in K$.

PROOF. We know that e_G is the unique element of G such that $\forall g \in G(e_G g = g e_g = g)$.
So, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) = \varphi(e_G)$ Multiplying both sides by $\varphi(e_G)^{-1} \in H$
So $\varphi(e_G) = e_H$. □(C1)

CLAIM (2). $\forall g \in G \varphi(g^{-1}) = (\varphi(g))^{-1}$

PROOF. $\varphi(g^{-1})\varphi(g) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$ By symmetry, $\varphi(g)\varphi(g^{-1}) = e_H$ □(C2)

□(Prop.)

Lecture 9 (2016–02–03)

Class Note
Midterm 1 is on Friday February 26th (in class)

Last time: showed that the kernel of a homomorphism is a subgroup.

PROPOSITION 44. $K \trianglelefteq G$.

PROOF. First we show $K \leq G$.

- $K \neq \emptyset$ as $e_G \in K$.
- $\forall g_1, g_2 \in K, g_1 g_2 \in K$:
  $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e_H e_H = e_H$ So $g_1 g_2 \in K$
- $\forall g \in H, g^{-1} \in K$:
  $\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H$
  So $g^{-1} \in K$

Thus, $K \leq G$. Next, we prove. $\forall k \in K, \forall g \in G$:

$$\varphi(g^{-1}kg) = \varphi(g^{-1})\varphi(h)\varphi(g) = (\varphi(g))^{-1} e_H \varphi(g) = e_H$$

Hence $g^{-1}kg \in K$. □

Definition 45. If $\varphi : G \to H$ is a group homomorphism, and $h \in H$, the fiber above h is the set $\varphi^{-1}(\{h\})$.

Thus, $\mathrm{Ker}(\varphi)$ is the fiber above e_H.

Example.

- $\varphi(\mathbb{R},+) \to (\mathbb{R}^+,\times)$, $\varphi(r) = \mathrm{e}^r$ φ is a homomorphism since $\varphi(r+s) = \mathrm{e}^{r+s} = \mathrm{e}^r\mathrm{e}^s = \varphi(r) \times \varphi(s)$
  $\mathrm{Ker}(\varphi) = \{r \in R : \varphi(r) = 1\} = \{0\}$.
  The fiber above $s \in \mathbb{R}^+$: $\varphi(r) = s \iff \mathrm{e}^r = s \iff r = \ln s$. Thus $\varphi^{-1}(\{s\}) = \{\ln s\}$.
- $\varphi : (\mathbb{C} \setminus \{0\}, \times) \to (\mathbb{R} \setminus \{0\}, \times)$, $\varphi(a + b\mathrm{i}) = a^2 + b^2$.
  φ is a homomorphism (verification left to the reader).
  $\mathrm{Ker}(\varphi) = \{a+b\mathrm{i} : \varphi(a+b\mathrm{i}) = 1\} = \{a+b\mathrm{i} : a^2+b^2 = 1\}$, which is the unit circle in the complex plane.
  Fix $r \in \mathbb{R} \setminus \{0\}$, lets examine the fiber above r:
  $$\{a + b\mathrm{i} : a^2 + b^2 = r\} = \begin{cases} \emptyset & \text{if } r < 0 \\ \text{Circle of radius } \sqrt{r} & \text{if } r > 0 \end{cases}$$
- Start with a group G, normal $N \trianglelefteq G$. $\varphi : G \to G/N$, $\varphi(g) = gN$ is a homomorphism.

  Proof. $\varphi(g_1g_2) = (g_1g_2)N = (g_1N)(g_2N) = \varphi(g_1)\varphi(g_2)$ □

  $\mathrm{Ker}(\varphi) = \{g : \varphi(g) = eN\} = \{g : \varphi(g) = eN\} = N$.

This leads us to the realization that:

Proposition 46. *$N \trianglelefteq G \iff N = \mathrm{Ker}(\phi)$ for some homomorphism $\varphi : G \to H$, for any group H.*

Why do all fibers look alike?

Proposition 47. *If $\phi : G \to H$ is a group homomorphism and $h \in H$, then $\varphi^{-1}(\{h\})$ is either $\emptyset$ or gK for some $g \in G$, where $K = \mathrm{Ker}(\varphi)$*

Proof. If $\nexists g \in G$ such that $\varphi(g) = h$ then $\varphi^{-1}(\{h\}) = \emptyset$.
Else, fix some $g \in G$ such that $\varphi(g) = h$.

Claim (1). *$gK \supseteq \varphi^{-1}(\{h\})$*

Proof. Suppose $g' \in \varphi^{-1}(\{h\})$ (i.e. $\varphi(g') = h$). Want $g' \in gK$. So, $\varphi(gg'^{-1}) = \varphi(g)\varphi(g'^{-1}) = \varphi(g)\varphi(g')^{-1} = hh^{-1} = e_H$. Hence $gg'^{-1} \in K$, so $g' \sim g \pmod K$, so $g' \in gK$. □(C1)

Claim (2). *$gK \subseteq \varphi^{-1}(\{h\})$*

Proof. Suppose $g' \in gK$, want $\varphi(g') = h$. Fix $k \in K$ such that $g' = gk$. $\varphi(g') = \varphi(gk) = \varphi(g)\varphi(k) = he_H = h$. □(C2)

Thus, $gK = \varphi^{-1}(\{h\})$, as desired. □(Prop.)

Corollary 48. *If $\varphi : G \to H$ is a group homomorphism, the following are equal:*

- *φ is injective.*

- $\mathrm{Ker}(\varphi) = \{e_G\}$

DEFINITION 49. A map $\varphi : G \to H$ between groups is an isomorphism if it is a bijective homomorphism. We often say $G \cong H$ if there exists an isomorphism $\phi : G \to H$.

Intuition: Isomorphic groups have the "same operation" on different sets.

EXAMPLE. Let $G = \{a, b\}$ $\begin{array}{c|cc} & a & b \\ \hline a & a & b \\ b & b & a \end{array}$ Then, $G \cong \mathbb{Z}/2\mathbb{Z}$ via $\varphi : a \mapsto \overline{0}, b \mapsto \overline{1}$

We know $\varphi : G \to H$ is an isomorphism if it's a homomorphism, surjective, and $\mathrm{Ker}(\varphi) = \{e_G\}$.

Lecture 10 (2016–02–06)

DEFINITION 50. If $\varphi : G \to H$ is a function, denote by $\mathrm{Im}(\varphi)$, or $\varphi(G)$, or $\varphi[G]$ the image of G, i.e., the set $\{h \in H, \exists g \in G : \varphi(g) = h\}$.

EXERCISE. Prove: If $\varphi : G \to H$ is a group homomorphism then $\varphi[G] \leq H$.

THEOREM 51 (First Isomorphism Theorem). *If $\varphi : G \to H$ is a group homomorphism, then $\varphi[G] \cong G/\mathrm{Ker}(\varphi)$.*

PROOF. Abbreviate $I := \varphi[G], K := \mathrm{Ker}(\varphi)$. We know for $h \in I$: $\varphi^{-1}(\{h\}) \neq \emptyset$. Hence, $\varphi^{-1}(\{h\}) = gK$ for some $gK \in G/K$. Then, define $\psi : I \to G/K$. $\psi(h) = \varphi^{-1}(\{h\}) = gK$.

CLAIM. $\psi : I \to G/K$ is a group isomorphism.

PROOF. We show that ψ is a bijective homomorphism in three parts:

(a) ψ is a homomorphism:
Fix $h_1, h_2 \in I$, want $\psi(h_1, h_2) = \psi(h_1)\psi(h_2)$. Fix g_1, g_2 such that $\varphi(g_1) = h_1, \varphi(g_2) = h_2$. Then $\varphi(g_1 g_2) = h_1 h_2$ by def of homomorphism. So, $\psi(h_1 h_2) = g_1 g_2 K = (g_1 K)(g_2 K) = \psi(h_1)\psi(h_2)$. $\square$(a)

(b) ψ is a surjection:
Fix $gK \in G/K$. Want $h \in I$ with $\psi(h) = gK$ Want $h \in I$ with $\psi(h) = gK$. Choose $h \in \psi(g)$. Then by def, $g \in \varphi^{-1}(\{h\})$. Thus, $\psi(h) = \varphi^{-1}(\{h\}) = gK$. $\square$(b)

(c) ψ is an injection:
As remarked, it suffices to show

$$\mathrm{Ker}(\psi) = \{h \in I : \psi(h) = \underbrace{e_G K}_{=e_{G/K}}\} = \{h \in I : \varphi^{-1}(\{h\})\} = \{h \in I : \varphi(e_G) = h\} = \{e_H\}$$

$\square$(c)

$\square$(Claim)

$\square$(Thm)

DEFINITION 52. A group G is cyclic if $\exists x \in G : \langle x \rangle = G$. (Where $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$.)

PROPOSITION 53. *If G is a cyclic group, then $G \cong \mathbb{Z}$, or $G \cong (\mathbb{Z}/n\mathbb{Z})$ for some $n \in \mathbb{Z}$.*

PROOF. As G is cyclic, take $x \in G$ such that $\langle x \rangle = G$. the map $\varphi : (\mathbb{Z}, +) \to G$, $\varphi(n) = x^n$. By hypothesis, $\langle x \rangle = G$. φ is surjective, so $\mathrm{Im}(\varphi) = G$. By first isomorphism theorem, $G \cong (\mathbb{Z}/\mathrm{Ker}(\varphi))$.

Assume $\nexists n > 0$ such that $x^n = 1_G$ (i.e., the order of x in G is infinite.) Then $\operatorname{Ker}(\varphi) = \{n \cdot x^n = e_G\} = \{0\}$. Also $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ (proof left as exercise). Thus, $G \cong \mathbb{Z}$.
Otherwise, fix the least $n > 0$ such that $x^n = e_G$(so $n = |x|$).
Check (exercise): $\operatorname{Ker}(\varphi) = \{m \in \mathbb{Z} : x^m = e_G\} = n\mathbb{Z}$. Thus $G \cong \mathbb{Z}/\operatorname{Ker}(\varphi) = \mathbb{Z}/n\mathbb{Z}$. $\square$

COROLLARY 54. *Suppose $p > 1$ is prime and G is a group with $|G| = p$. Then $G \cong (\mathbb{Z}/p\mathbb{Z})$.*

PROOF. Fix any $x \in G$, $x \neq e^G$. $|x| \neq 1$. Additionally $|x|$ divides $|G|$. Thus $|x| = p$, as p is prime. Then $\langle x \rangle = G$. $\square$

Our next big motivational question: Given $n \in \mathbb{N}$, can we "classify" (or list) all groups of cardinality n (up to $\cong$)?
What we know so far:

n	Groups:
0	None
1	{e}
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}, \ldots ?$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}, \ldots ?$

DEFINITION 55. G, H are groups, build a group of the direct product of G and H, denoted $G \times H$ with underlying set $\{(g, h) : g \in G, h \in H\}$, and group operation $(g_1, h_1) \cdot (g_2, h_2) = ((g_1 \cdot_G g_2), (h_1 \cdot_H h_2))$

PROPOSITION 56. *If $|G| = 2$ then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$*

Lecture 11 (2016–02–08)

PROPOSITION 57. *Suppose G is a group. Then $G/\{e_G\} \cong G$ and $G/G \cong \{e_G\}$.*

PROOF. Consider the homomorphism $\varphi : G \to G$ with $\varphi(g) = g$ $\operatorname{Ker}(\varphi) = \{g \in G : \varphi(g) = e_G\} = \{e_G\}$, and $\varphi[G] = G$.
Thus, the first isomorphism theorem states that $G/\operatorname{Ker}(G) \cong \varphi[G]$.
Next, consider the homomorphism $\psi : G \to G$, $\psi(g) = e_G$. Then $\operatorname{Ker}(\psi) = G$, $\operatorname{Im}(\psi) = \{e_G\}$.
By the first isomorphism theorem, $G/G \cong \{e_G\}$. $\square$

Groups of cardinality 4.

PROPOSITION 58. *If G is a group with $|G| = 4$ then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.*

We note that the above groups are not isomorphic because there is no element of order 4 in $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

PROOF. Possible orders for elements are 1, 2, or 4.
Two cases:

(1) $\exists g \in G, |g| = 4$ then $G = \langle g \rangle$, so (as proved last time) $G \cong (\mathbb{Z}/4\mathbb{Z})$.
(2) $\nexists g \in G, |g| = 4$:
So $G = \{e_G, a, b, c\}$, meaning $|e_G| = 1$ and $|a| = |b| = |c| = 2$. So $\forall g \in G(g^2 = e_G)$. Hence G is abelian (Homework). What is ab? It's not e_G as $a^{-1} = a \neq b$. It's not a since $b \neq e_G$. It's not b since $a \neq e_G$. So $ab = c$. Thus we may write the multiplication table.

Verification that $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is left to the reader.

$\square$

REMARK. More generally, if p prime and $|G| = p^2$ then $G \cong (\mathbb{Z}/p^2\mathbb{Z})$ or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

PROPOSITION 59. *Suppose G is a group and $|G| = 6$. Then $G \cong (\mathbb{Z}/6\mathbb{Z})$ or $G \cong S_3$.*

PROOF. (Sketch)
If $\exists x \in G$ with $|x| = G$ then $G = \langle x \rangle \cong (\mathbb{Z}/6\mathbb{Z})$.
More subtly, if $\exists a, b \in G$ such that $|a| = 3$ and $|b| = 2$ and $ab = ba$ then $G \cong (\mathbb{Z}/6\mathbb{Z})$ (verification that $|ab| = 6$ left as an exercise to the reader).
WLOG, assume all non-identity elements have order 2 or 3.
Also, elements of order 3 come in pairs. $|x| = 3, |x^{-1}| = 3, x \neq x^{-1}$. So $|\{x : |x| = 3\}| \in \{0, 2, 4\}$ (as it must be even, and $|e_G| = 1 \neq 3$).
Possible order breakdowns: either (A): 1 2 2 2 2 2 2, (B): 1 2 2 2 3 3, or (C): 1 2 3 3 3 3.

CLAIM (1). (A) can't happen. Why? Assume otherwise, then $\forall x \in G(x^2 = e)$ so G is abelian, so $\{1, a, b, ab\}$ is a subgroup, but $4 \not| 6$. so by Lagrange's theorem, this cannot happen.

CLAIM (2). (C) also cannot happen. Why? Assume otherwise, then denote by x the unique element of order 2. Then, $\forall g \in G, g^{-1}xg$ also has order 2. as

$$g^{-1}xgg^{-1}xg = g^{-1}x^2g = g^{-1}g = e$$

Thus, $g^{-1}xg$ has order 2. $\forall g \in G$, $g^{-1}xg = x \implies xg = gx$, contradiction.

CLAIM (3). (B) forces $G \cong S_3$. Proof of this follows from brute force considering the multiplication table.

$\square$(outline)

Group Actions

"Groups, like men, shall be judged by their actions." – Unknown

Definition 60. Suppose G is a group (not necessarily finite), and X is a set (also not necessarily finite). A group action of G on X is formally a function $a : G \times X \to X$ such that $\forall x \in X : a(e_G, x) = x$, and $\forall g, h \in G, x \in X : a(gh, x) = a(g, a(h, x))$.

Notation. We write actions like this: $G \curvearrowright X$ "G acts on X," and $g \cdot x := a(g, x)$.
The conditions then become $e_G \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$.

Equivalently, instead of thinking about an action as a function of $(G \times X) \to X$, you can view it as a ("curried") function of $G \to (X \to X)$.
Say $g \mapsto \sigma_g$ where $\sigma_g \cdot (X \to X)$ is defined by $\sigma_g(x) = g \cdot x = a(g, x)$.

Claim. $\forall g \in G, \sigma_g$ is a permutation of X.

Proof. $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{g^{-1}} \circ \sigma_g = \sigma_{e_G} (= x \mapsto x)$.
Why?

$$\sigma_g \circ \sigma_{g^{-1}}(x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e_G \cdot x = x = \sigma_{e_G}(x)$$

Thus, σ_g is a bijection. $\square$

An action then induces a map $G \to S_X$, $g \mapsto \sigma_g$. Note that $\sigma_g \circ \sigma_h = \sigma_{gh}$.

Property 61. Actions of G on X correspond to homomorphisms $G \to S_X$.

Example. Of actions:

(1) $X = \{1, 2, \ldots, n\}, S_n \curvearrowright X$ The action is $\sigma \cdot x = \sigma(x)$.
More generally, if $H \leq S_n$, we get an analogous action.

(2) Let G be the 2×2 invertible matrices over $\mathbb{R}$ under the operation of matrix multiplication.
$G \curvearrowright \mathbb{R}^2$ (acts on the Euclidean plane) by applying the matrices' corresponding linear transformation to the vector in $\mathbb{R}^2$. (Verification left to the reader.)

(3) $G = (\mathbb{R}, +)$ X is a circle. $G \curvearrowright X$ r "rotates the circle r radians c.c.w."

Lecture 12 (2016–02–10)

Note: group actions can be either left actions or right actions. However, we will only talk about left actions in this course, so we will refer to them exclusively as "actions."
Alternate def $G \to S_X$.
Important special case: $X = G$, then $G \curvearrowright G$ (G acts on itself).
There are three main actions:

- $G \curvearrowright G$ by left multiplication. $\forall g \in G, x \in X (= G), g \cdot x = gx$.
- $G \curvearrowright G$ by right multiplication. $g, x \in G, g \cdot x = xg^{-1}$.

- $G \curvearrowright G$ by conjugation. $g \cdot x = gxg^{-1}$. Note that gxg^{-1} is simply x conjugated by g^{-1}, so it doesn't matter whether we write $g^{-1}xg$ or gxg^{-1}.

THEOREM 62 (Cayley). *Suppose G is a group. Then there is a set X and a subgroup $H \leq S_X$ such that $G \cong H$.*
Moreover, we can choose X to have cardinality $|G|$. (i.e., if $|G| = n$, we can find an isomorphic copy of G inside S_n.)

PROOF. Take $X = G$ and consider the action $G \curvearrowright G$ by left multiplication ($g \cdot x = gx$). This induces a homomorphism $\varphi : G \to S_G, \varphi(g) = \lambda_g$ where $\lambda_g(x) = gx$.

CLAIM. $\mathrm{Ker}(\varphi) = \{e_G\}$.

PROOF (CLAIM): Suppose $g \in G$ such that $\varphi(g) = e \in S_G$. so $\lambda_g = e$.
In particular, $e_G = \lambda_g(e_G) = ge_G = g$, so $g = e_G$. □(Claim)

By the first isomorphism theorem, $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$. Denote by H the image of φ. $H \leq S_G$.
$G/\mathrm{Ker}(\varphi) = G/\{e_G\} \cong G$, so $G \cong H$. □(Theorem)

EXAMPLE. A concrete example:
$G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{1, a, b, c\}$

$$\lambda_b : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 4 \\ 3 \mapsto 1 \\ 4 \mapsto 2 \end{cases} \quad \text{Run cycle decomposition on each}$$

$G \cong \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4), (2\ 3)\} \leq S_4$.
This is sometimes called the left multiplication permutation representation of a group.

REMARK. Cayley's theorem is not always "optimal." Sometimes $|G| = n$ and $m < n$ such that $H \leq S_m$ and $G \cong H$.

EXAMPLE. $(\mathbb{Z}/6\mathbb{Z}) = G, |G| = 6$. Take $\sigma = (1\ 2\ 3)(4\ 5) \in S_5$.
Then $H = \langle\sigma\rangle \cong (\mathbb{Z}/6\mathbb{Z}) = G$, but $H \leq S_5$ and $5 < 6$.

Orbit Equivalence Relations

Definition 63. Suppose $G \curvearrowright X$. Define a relation $\sim$ on X by $x \sim y$ iff $\exists g \in G : g \cdot x = y$. This $\sim$ is called the orbit equivalence relation.

Proposition 64. *$\sim$ is an equivalence relation.*

Proof. 3 properties:

- Reflexivity:
  $x \in X$. $e_G \cdot x = x$, so $x \sim x$
- Symmetry:
  Suppose $x \sim y$. Fix $g \in G$ such that $g \cdot x = y$. Compute $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (gg^{-1}) \cdot x = e_G \cdot x = x$. So $y \sim x$
- Transitivity:
  Suppose $x \sim y, y \sim z$. Fix $g, h \in G$ such that $g \cdot x = y$ and $h \cdot y = z$. So $(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z$, so $x \sim z$

It follows that $\sim$ is an equivalence relation. $\square$

Definition 65. The equivalence classes of $\sim$ are called orbits. Write them like $\mathcal{O}_x$. Because $\sim$ is an equivalence class, $\{\mathcal{O}_x\}_{x \in X}$ partitions X.

Notation. Sometimes we write $G \cdot x$ to denote the orbit of x.

Lecture 13 (2016–02–12)

Definition 66. $G \curvearrowright X$, fix $x \in X$. The stabilizer of x is $G_x = \{g \in G : g \cdot x = x\} \subseteq G$.

Proposition 67. *If G is a group then $G_x \leq G$.*

Proof. Homework Question $\square$

Example. Let's look at some examples of group actions and stabilizers of some the elements of the sets they act on.

(1) $\sigma \in S_5$, say $\sigma = (1\ 3\ 4)(2\ 5)$. $S_5 \curvearrowright \{1, 2, 3, 4, 5\}$. This induces an action of $\langle\sigma\rangle \curvearrowright \{1, 2, 3, 4, 5\}$. (Note that $|\sigma| = 6$.)

   $G = \langle\sigma\rangle = \{e, \sigma, \ldots, \sigma^5\}$. $X = \{1, 2, 3, 4, 5\}$. Look at $x = 3$. $\mathcal{O} = \{1, 34\}$ = the cycle containing 3 in the cycle decomposition of σ.

   If we check each exhaustively, we find $e \cdot 3 = 3$ and $\sigma^3 = 3$ so the stabilizer of G_3 is $\{e, \sigma^3\}$.

   In general, if you have any perm group, the orbit of an element of the cyclic subgroup generated by an element in the permutation group is going to be the cycles and the stabilizers are going to be the lengths of the cycles.

(2) $G \curvearrowright G$ by left multiplication. $g \cdot x = gx$

   Claim. $\forall x \in G$, $\mathcal{O}_x = G$ (its orbit is G).

PROOF. Fix $x \in G$, Fix $g \in G$. Choose $h = gx^{-1}$, then $h \cdot x = (gx^{-1}) \cdot x = (gx^{-1})x = g(x^{-1}x) = g$. Thus, $g \in \mathcal{O}_x$. Thus, $\mathcal{O}_x = G$. □

CLAIM. $\forall x \in G, G_x = \{e_G\}$.

PROOF. Fix x. Suppose $g \in G$. $g \cdot x = x$.
Thus, $gxx^{-1} = xx^{-1}$ (as $X = G$), so $g = e_G$. □

(3) $S_3 \curvearrowright S_3$ by conjugation. $g \cdot x = gxg^{-1}$.
Orbits $\{e\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$
The stabilizer of $(1\ 2)$ is $\{e, (1\ 2)\}$.

(4) $H \leq G$. Let $H \curvearrowright G$ by right multiplication. Then

$$\mathcal{O}_{x \in G} = \{h \cdot x : h \in H\} = \{xh^{-1} : h \in H\} = \{xh : h \in H\} = xH.$$

Thus, the orbits of the elements of G are the left cosets of H in G.

DEFINITION 68. Suppose $G \curvearrowright X$ with a single orbit $\mathcal{O} = X$.
We say that the action is transitive

DEFINITION 69. Orbits of the conjugation action of $G \curvearrowright G$ are called conjugacy classes.

THEOREM 70 (Orbit-Stabilizer Theorem). *Suppose G is a finite group, X is some set, and $G \curvearrowright X$. Fix arbitrarily $x \in X$ with orbit $\mathcal{O} \subseteq X$ and stabilizer $G_x \leq G$. Then $|\mathcal{O}| \cdot |G_x| = |G|$.*

PROOF. Define two equivalence relations on G.

(1) $g \sim h$ iff $g^{-1}h \in G_x$ (left coset equivalence of stabilizers)
(2) $g \approx g$ iff $g \cdot x = h \cdot x \in X$

For the reader: check $\sim$ and $\approx$ are equivalence relations.

CLAIM (1). Each $\sim$ equivalence class has $|G_x|$ many elements in it.

PROOF. Already done □(Claim 1)

CLAIM (2). There are exactly $|\mathcal{O}|$-many $\approx$ equivalence classes.

PROOF. For each $y \in \mathcal{O}$, put $A_y = \{g \in G : g \cdot x = y\}$. The collection of $\{A_y : y \in \mathcal{O}\}$ is exactly the set of $\approx$-equivalent classes.
In other words, $\approx$ is partitioning G by the elements which move x into each particular element of $\mathcal{O}$. □(Claim 2)

CLAIM (3). $\sim \cong \approx$

PROOF. First show $g \sim h \implies g \approx h$, then show $g \approx h \implies g \sim h$.

- Suppose $g^{-1}h \in G_x$, then $(g^{-1}h) \cdot x = x$, so $g^{-1} \cdot (h \cdot x) = x$.
  Act by g on both sides. $g \cdot x = g \cdot (g^{-1} \cdot (h \cdot x)) = (gg^{-1}) \cdot (h \cdot x) = h \cdot x$, so $g \approx h$.
- Suppose $g \cdot h = h \cdot x$. Act by g^{-1} on both sides. $g^{-1} \cdot (g \cdot h) = g^{-1}(h \cdot x)$.
  $x = e_G \cdot x = (g^{-1}h) \cdot x$, thus $g^{-1}h \in G_x$.

□(Claim 3)

So the upshot is that we have a single equivalence relation on G. It has $|\mathcal{O}|$ -many classes. Each class has $|G_x|$-many elements. Hence $|G| = |\mathcal{O}| \cdot |G_x|$. □(Theorem 70)

REMARK. The above theorem also works when G is not finite, however it involves multiplication of ordinals, which is beyond the scope of this course.

Lecture 14 (2016–02–15)

We will continue referencing the Orbit-Stabilizer Theorem for the rest of the week

Example. Fix $p \geq 2$ prime and $c \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. How many distinct (up to rotation) necklaces can you make of length p out of c colors of beads?
More formally, let $X = \{$sequences of length p with entries in $\{1, 2, \ldots, c\}\}$. Also, let $G = (\mathbb{Z}/p\mathbb{Z})$ act on X by "rotating the indices" $\pmod p$.
For example, if $x = (1, 2, 1, 2, 3) \in X$, then $\overline{1} \cdot x = (3, 1, 2, 1, 2), \overline{3} \cdot x = (1, 2, 3, 1, 2)$.
Question: How many orbits does this action have?
We know by the Orbit-Stabilizer Theorem that for any $x \in X$, $|\mathcal{O}_x| \cdot |G_x| = |G| = p$. Thus $\{|\mathcal{O}_x|, |G_x|\} = 1, p$. Thus, let us pick an arbitrary necklace $x \in X$ and examine $\mathcal{O}_x$ and G_x.

Case 1: $|\mathcal{O}_x| = 1$. Then $|G_x| = p$. So $g \cdot x = x$ for *all* $g \in (\mathbb{Z}/p\mathbb{Z})$. This necessitates that every bead in x is the same as the next one, meaning all the beads on x are the same color. As there are c colors, there are exactly c-many possible distinct $x \in X$ in this case.

Case 2: $|\mathcal{O}_x| = p$. Then $|G_x| = 1$. All other $x \in X$ fall into this case. $|X| = c^p$ as there are p places with c choices each. Thus there are $c^p - c$ necklaces falling into this case.

Thus, the total number of orbits is $c + \frac{c^p - c}{p}$. As a nice corollary, this implies that $\frac{c^p - c}{p}$ is an integer, as it is counting something.

Next, we make necklaces out of group elements.

Theorem 71 (Cauchy). *Suppose that G is a finite group $|G| = n$ and $p \geq 2$ is a prime such that $p|n$. Then $\exists g \in G$ such that $|g| = p$.*

Proof. Let X be the set of sequences $(g_1, g_2, \ldots, g_p)$ of length p with elements from G, such that $\prod_{i=1}^{p} g_i = e_G$.

Claim (1). $|X| = n^{p-1}$

Proof. Fix $g_1, \ldots, g_{p-1}$. Then $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$ is the unique way to land in X. $\square$(C1)

Claim (2). Suppose $(g_1, g_2, \ldots, g_p) \in X$. Then $(g_p, g_1, g_2, \ldots g_{p-1}) \in X$.

Proof. We know $\prod_{i=1}^{p} g_i = e_G$. Multiplying both sides on the right by g_p^{-1} gives $\prod_{i=1}^{p-1} g_i = g_p{}^{-1}$. Then, we multiply on the left by g_p. to get $g_p \prod_{i=1}^{p-1} g_i = e_G$. Note that this is simply conjugating by g_p. $\square$(C2)

Let $H = (\mathbb{Z}/p\mathbb{Z})$, $H \curvearrowright X$ by "rotation." So, $\overline{1} \cdot (g_1, g_2, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$. By claim 2, we note that this is a group action. By the Orbit-Stabilizer Theorem , we have for every $x \in X, |\mathcal{O}_x| \cdot |H_x| = |H| = |(\mathbb{Z}/p\mathbb{Z})| = p$. So for every $x \in X, \mathcal{O}_x = 1$ or p.
Let's say k_1 is the number of orbits of cardinality 1, and k_p is the number of orbits of cardinality p.
Hence, $1 \cdot k_1 + p \cdot k_p = |X| = n^{p-1}$, so $k - 1 = n^{p-1} - p \cdot k_p$. Thus $p|k$.

Claim (3). $k_1 \geq 1$.

Proof. $(\underbrace{e_G, e_G, \ldots, e_G}_{p \text{ times}}) \in X$ $\square$(C3)

Thus, by claim 3 and the fact that $p|k$, $k_1 \geq p$. In particular, $k_1 \geq 2$. So there is some $x \in X$ with $x \neq (e_G, e_G, \ldots, e_G)$ such that $\mathcal{O}_x = 1$. So $x = (\underbrace{g, g, \ldots, g}_{p \text{ times}})$ with $g \neq e_G$. $x \in X \implies \prod_{i=1}^{p} g = e_G \implies g^p = e_G$. Thus $|g| = p$, so we're done. □(Cauchy)

Remark. The above theorem is *false* if p were to be composite.

Lead in to next lecture: Conjugation.
Let $G \curvearrowright G$ by conjugation. $\forall g \in G, \forall x \in G : g \cdot x = gxg^{-1}$
If $x \in G$, what is G_x (under conjugation)?

$$G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

In other words, $G_x = \{g \in G : g \text{ commutes with } x\}$.

Definition 72. The center of G, denoted $Z(G)$ is the set $\{x \in G : \forall g \in G(gx = xg)\}$.

So $x \in Z(G) \iff G_x = G$ (for conjugation). This is also equivalent to saying $\mathcal{O}_x = \{x\}$.

Lecture 15 (2016–02–17)

Class Note

Midterm coming up: February 26th in class (1:30-2:20pm)
Class Plans: Up to spring break, we'll continue talking about groups
After spring break, we'll start ring theory.

Definition 73. $G \curvearrowright X$ $x \in X$ is a fixed point of the action if $\forall g \in G(g \cdot x) = x$. (This is equivalent to saying $G_x = G$, or $\mathcal{O}_x = \{x\}$.)

Example.

(A) $(\mathbb{Z}/n\mathbb{Z})$ acts by "rotation" on "c^n" = sequences of length n with elements in $\{1, 2, \ldots, c\}$. Then the fixed points are the constant sequences.
(B) $G \curvearrowright G$ by left or right multiplication and $G \neq \{e_G\}$, then there are *no* fixed points. (Take $g \neq e_G$, then $g \cdot h = gh \neq h$.)
(C) $G \curvearrowright G$ by conjugation. $g \cdot x = gxg^{-1}$. Then x is a fixed point iff $x \in Z(G)$, i.e., $\forall g \in G(xg = gx)$, x commutes with everything in G.

Definition 74. Given a prime $p \geq 2$, we say that a finite group G is a p-group if $|G| = p^k$ for some $k \in \mathbb{N}^+$.

Proposition 75. *The following are equivalent:*

(1) G is a p-group
(2) Every subgroup $H \leq G$ is a p-group
(3) Every $g \in G$ has $|g| = p^i$ for some $i \in \mathbb{N}$

Proof. Left to the reader. □

Theorem 76 (Fixed-Point Lemma). *Suppose p prime, G is a p-group and $G \curvearrowright X$, and let F be the number of fixed points. Then, $F \equiv |X| \pmod{p}$.*

PROOF. Say $|G| = p^k$. By the Orbit-Stabilizer Theorem, for $x \in X$, $|\mathcal{O}_x| \cdot |G_x| = p^k$. so $|\mathcal{O}_x| \in \{1, p, p^2, \ldots, p^k\}$.
For $0 \leq i \leq k$, denote by n_{p_i} the number of orbits of size p^i.

$$|X| = \sum_{i=0}^{k} p^i \cdot n_{p^i}$$

as the orbits partition X. Thus, $|X| - n_1 = \sum_{i=1}^{k} p^i \cdot n_{p^i}$, so $p|(|X| - n_1)$. It follows that $n_1 \equiv |X| \pmod{p}$, as desired. □(Lem)

COROLLARY 77. *Suppose p prime and $G \neq \{e\}$ is a p-group. Then $|Z(G)| \geq p$.*

PROOF. $|Z(G)|$ = number of fixed points of $G \curvearrowright G$ by conjugation. Thus, by the Fixed-Point Lemma, $|Z(G)| \cong |G| \pmod{p}$. So, $|Z(G)|$ is a multiple of p.

CLAIM. $|Z(G)| \neq 0$. This is true as $e_G \in Z(G)$.

Thus, $|Z(G)| \geq p$. □(Cor)

PROPOSITION 78. *Suppose p prime, G is a group with $|G| = p^2$. Then, $G \cong (\mathbb{Z}/p^2\mathbb{Z})$ OR $G \cong ((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}))$.*

PROOF. If $\exists g \in G$ with $|g| = p^2$ then $\langle g \rangle = G$, so $G \cong (\mathbb{Z}/p^2\mathbb{Z})$.
Otherwise, all non-identity elements of G have order p.
Since $|Z(G)| \geq p \geq 2$, we may fix non-identity $h \in Z(G)$ The set $\langle h \rangle$ has cardinality p. Now pick $k \in G \setminus \langle h \rangle$. Put $H := \langle h \rangle$ and $K := \langle k \rangle$, both with cardinality p.

CLAIM. The map $\varphi : ((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})) \to G$ with $\varphi(\bar{i}, \overline{m}) = h^i k^m$ is an isomorphism. ($\bar{i}$ and $\overline{m}$ are residue classes of $(\mathbb{Z}/p\mathbb{Z})$.) Note that if $i, j \in \bar{i}$, then $h^i = h^j$, so $h^i (h^j)^{-1} = h^{i-j} = h^{pa} = e_G$.

PROOF. First we show φ is a homomorphism, i.e., $\varphi(\bar{i} + \bar{j}, \overline{m} + \overline{n}) = (h^i k^m)(h^j k^n) = \varphi(\bar{i}, \overline{m})\varphi(\bar{j}, \overline{n})$.
It is apparent that $\varphi(\bar{i} + \bar{j}, \overline{m} + \overline{n}) = h^{i+j} k^{m+n} = h^i h^j k^m k^n$. However, as h is in the center of G, h and k commute, so $h^i h^j k^m k^n = h^i k^m h^j k^n$ as desired.
Next we show that φ is an isomorphism by showing it is also a bijection.
Since $|((\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}))| = |G| = |p^2|$, to show φ is bijective, it suffices to show that φ is *injective*. In turn, it is sufficient to prove $\mathrm{Ker}(\varphi) = \{e_G\}$.
As we proved in a homework, $H \cap K \leq H$, so $|H \cap K|$ is 1 or p. $k \notin H \cap K$, so $|H \cap K| \lneq |K|$. Thus, as the cardinality of the intersection must divide p^k, the intersection has cardinality 1, meaning $H \cap K = \{e_G\}$
Suppose $\bar{i}, \overline{m} \in (\mathbb{Z}/p\mathbb{Z})$ with $\varphi(\bar{i}, \overline{m}) = e_G$. Then $h^i k^m = e_G$. Thus, $\underbrace{h^i}_{\in H} = \underbrace{k^{-m}}_{\in K}$. Since $h^i = k^{-m} \in H \cap K$, $h^i = k^{-m} = e_G$. So i, m are multiples of p. Hence, $(\bar{i}, \overline{m}) = (\bar{0}, \bar{0})$. Thus $\mathrm{Ker}(\varphi) = \{e_G\}$, so φ is injective as desired, meaning φ is an isomorphism. □(prop)

□

Lecture 16 (2016–02–19)

Class Note

Review sheet for Midterm 1 will be posted this afternoon.
(Exam on February 26th in class).

Conjugation in S_n.

Example. Suppose $\sigma = (1\ 3\ 4)(2\ 5) \in S_5$ and $\tau = (1\ 2\ 3\ 4\ 5) \in S_5$. What is $\tau\sigma\tau^{-1}$?
Compute $\tau^{-1} = (1\ 5\ 4\ 3\ 2)$.
So, $\tau\sigma\tau^{-1} = (1\ 2\ 3\ 4\ 5)(1\ 3\ 4)(2\ 5)(1\ 5\ 4\ 3\ 2) = (1\ 3)(2\ 4\ 5)$

Proposition 79. *Suppose $\sigma, \tau \in S_n$. Fix $a, b \in \{1, 2, \ldots, n\}$. Supose $\sigma' := \tau\sigma\tau^{-1}$. If $\sigma(a) = b$ then $\sigma'(\tau(a)) = \tau(b)$*

Proof. $\sigma'(\tau(a)) = (\tau\sigma\tau^{-1}\tau)(a) = (\tau\sigma)(a) = \tau(b)$. □

But why is this useful? Conjugation in S_n is "relabeling." Revisiting the previous example: $\sigma = (1\ 3\ 4)(2\ 5)$ $\tau\sigma\tau^{-1} = (\tau(1)\ \tau(3)\ \tau(4))(\tau(3)\ \tau(5)) = (2\ 4\ 5)(3\ 1) = (1\ 3)(2\ 4\ 5)$.
We've shown: Whenever σ, σ' are conjugate in S_n, then σ, σ' have the same cycle type (i.e. the same number of cycles of each length).

Definition 80. The cycle type of a permutation is the number of cycles of each length in the permutation's cycle decomposition

Theorem 81. *$\sigma, \sigma' \in S_n$ are conjugate (in S_n) if and only if they have the same cycle type.*

Sketch. We know that conjugate $\implies$ same cycle type. For the converse, suppose σ, σ' have the same cycle type.
Shuffle the cycles (because they're disjoint) in σ to line up with those of σ.
Then take the permutation that takes the elements in the cycles of σ to the corresponding elements in the cycles of σ'. (Also, make sure that fixed points are sent to fixed points.)
This generates a permutation τ such that $\tau\sigma\tau^{-1} = \sigma'$, so σ and σ' are conjugate. □(sketch)

Example. $\sigma = (1\ 3)(2\ 5\ 6)(4\ 7) \in S_7$ $\sigma' = (1\ 5\ 7)(2\ 3)(4\ 6) \in S_7$.
Thus, by our last theorem, they are conjugate.
Shuffle σ' to corespond with σ:
$\sigma = (1\ 3)(2\ 5\ 6)(4\ 7)$
$\sigma' = (2\ 3)(1\ 5\ 7)(4\ 6)$
Thus, $\tau = (1\ 2)\cancel{(3)}\cancel{(4)}\cancel{(5)}(6\ 7)$.
Note that we could have shuffled the cycles differently and come up with a different τ.

Example. Compute the size of every conjugacy class in S_4. (Where the conjugacy classes are the orbits of $S_4 \curvearrowright S_4$ by conjugation).
By our previous theorem we only have to check each cycle type.

Cycle Types:	How many with that type?
$(\cdot\ \cdot\ \cdot\ \cdot)$	$3! = 6$
$(\cdot\ \cdot\ \cdot)$	$\binom{4}{3} \cdot 2! = 8$
$(\cdot\ \cdot)\ (\cdot\ \cdot)$	$\binom{4}{2} \cdot \binom{2}{2} \cdot \frac{1}{2!} \cdot 1! \cdot 1! = 3$
$(\cdot\ \cdot)$	$\binom{4}{2} \cdot 1! = 6$
e	1
Total:	24

Example. How many elements of S_5 commute with $\sigma = (1\ 4)(3\ 5)$? Use the Orbit-Stabilizer Theorem!
$S_5 \curvearrowright S_5$ by conjugation. $\mathcal{O}_\sigma =$ the conjugacy class of σ.
$G_\sigma = \{g \in S_5 : g\sigma g^{-1} = \sigma\} = \{g \in S_5 : g\sigma = \sigma g\}$. The Orbit-Stabilizer Theorem says taht $|\mathcal{O}_\sigma| \cdot |G_\sigma| = |S_5|$ Thus, as $|\mathcal{O}_\sigma| = 15$ and $|S_5| = 120$ so $|G_\sigma| = \frac{120}{15} = 8$.

Example. How many elements of S_9 commute with $\sigma = (1\ 2)(3\ 4)(5\ 6)(7\ 8\ 9)$?
The size of σ's conugacy class is $n = \binom{9}{2}\binom{7}{2}\binom{5}{2}\frac{1}{3!}1!1!1!2!$
Thus, the number of elements of S_9 commuting with σ is $\frac{9!}{n} =$

Lecture 17 (2016–02–22)

Definition 82. If $A, B \subseteq G$, where G is a group (A and B not necessarily). Then put $AB := \{ab : a \in A, b \in B\}$. We note that unless the group is abelian, order still matters.
Caveat: If $H, K \leq G$ are subgroups, then HK is typically *not* a subgroup.

Proposition 83. *If G is a finite group and $H, H \leq G$ are subgroups, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.*

Proof. Note that $HK = \{hk : h \in H, k \in K\} = \bigcup_{h\in H} hK$. So $|HK| = n \cdot |K|$, where n is the number of left cosets of K meeting H.

Claim. For $h_1, h_2 \in H$: $h_1K = h_2K \iff h_1^{-1}h_2 \in H \cap K$

Proof. ($\implies$): If $h_1K = h_2K$, then by definition of coset equaliy, we know that $h_1^{-1}h_2 \in K$. As H is a subgroup of G, $h_1^{-1}h_2 \in H$ also.
($\Longleftarrow$): If $h_1^{-1}h_2 \in H \cap K$, it's in K, so $h_1K = h_2K$. □(Claim)

Note that $H \cap K \leq H$. So the number of cosets of $H \cap K$ in H is $\frac{|H|}{|H\cap K|}$. Thus, $n = \frac{|H|}{|H\cap K|}$, meaning that $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$, as desired. □

Remark. The proposition is especially useful when $H \cap K = \{e_G\}$. In this case, you get $|HK| = |H| \cdot |K|$. This happens, for example, when

- $|H|, |K|$ are relatively prime
- $|H| = |K| = p$ prime, and $H \neq K$.

Corollary 84. *Suppose G is a finite group, and $H, K \leq G$ such that*
(1) $|G| = |H| \cdot |K|$
(2) $H \cap K = \{1\}$.
(3) $\forall h \in K, \forall k \in K : hk = kh$.
Then $G \cong H \times K$.

Proof. Consider the map $\varphi : H \times K \to G$ with $\varphi((h, k)) = hk$.

Claim (1). φ is a homomorphism.

1. Suppose $(h_1, k_1), (h_2, k_2) \in H\times K$. First compute $\varphi((h_1, k_1)(h_2, k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$. Then compute

$$\begin{aligned}&\varphi((h_1, k_1))\varphi((h_2, k_2))\\&= (h_1k_1, h_2k_2)\\&= h_1(k_1h_2)k_2\end{aligned}$$

As $hk = kh$ by assumption

$$\begin{aligned} &= h_1h_2k_1k_2 \\ &= \varphi((h_1,k_1)(h_2,k_2)) \end{aligned}$$

So φ is a homomorphism. $\square$(C1)

Claim (2). φ is a bijection.

2. Node $|G| = |H| \cdot |K| = |H \times K|$, which are both finite. So, it suffices to show that φ is a surjection.
$\varphi[H \times K] = \{hk : h \in H, k \in K\} = HK$, and $|HK| = \frac{|H|\cdot|K|}{H\cap K}$. Thus $\mathrm{Im}(\varphi) = G$, so φ is surjective. $\square$(C2)

It follows that φ is an isomorphism, so $G \cong H \times K$ as desired. $\square$(Cor)

Theorem 85. *Suppose G is finite and $H, K \trianglelefteq G$, such that:*

- $|G| = |H| \cdot |K|$
- $H \cap K = \{e_G\}$

Then $G \cong H \times K$.

Proof. By corollary 84, it suffices to show that $\forall h \in H, \forall k \in K : hk = kh$. Consider $hkh^{-1}k^{-1}$ (called the commutator).

Claim (1). $hkh^{-1}k^{-1} \in H$

Which is proved by inserting parentheses as follows:

$$\underbrace{h}_{\in H}\underbrace{(kh^{-1}k^{-1})}_{\in H} \in H,$$

where the second containment holds because H is normal.

Claim (2). $hkh^{-1}k^{-1} \in K$. This is true because$(hkh^{-1})k^{-1} \in K$, as K is normal.

Thus, $hkh^{-1}k^{-1} \in H \cap K = \{e_G\}$. So, $hkh^{-1}k^{-1} = e_g \implies hk = kh$. $\square$(Thm)

Next, we act on the set of subgroups by conjugation.

Proposition 86. *Let G be a group $H \leq G$ a subgroup, $g \in G$. Then $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G. Moreover, $gHg^{-1} \cong H$.*

Proof. Put $H' = gHg^{-1}$.
H' is nonempty as $ge_Gg^{-1} = e_G \in H'$.
H' is closed under products because if $gh_1g^{-1}, gh_2g^{-1} \in H'$, then $(gh_1hg^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in H'$.
H' is closed under inverses as if $ghg^{-1} \in H$, then $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = ghg^{-1} \in H'$

Claim. $\varphi : H \to H'$, $\varphi(h) = ghg^{-1}$ is an isomorphism.

The proof is left as an exercise to the reader. $\square$

Hence, G acts on $\{H : H \leq G\}$ by conjugation $g \cdot H = gHg^{-1}$.
In addition, H is a fixed point of this action exactly when $H \trianglelefteq G$.

Lecture 18 (2016–02–24)

THEOREM 87. *Suppose $p < q$ primes and $q \not\equiv 1 \pmod p$. Then every group G with $|G| = pq$ is cyclic. (i.e., $G \cong (\mathbb{Z}/pq\mathbb{Z})$)*

PROOF. Let $p = 3, q = 5$, The general case proof is left as an exercise.
Note: $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ ic cyclic because $|(h, k)| = \operatorname{lcm}(p, q) = pq$ (as they're relatively prime).
So now there is enough to show that $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. By Cauchy, we may take subgroups $H, K \leq G$ with $|H| = p$ and $|K| = q$. We want: $\forall h \in H, \forall k \in K : hk = kh$ (then $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$).
First we let K act on the subgroups of G by conjugation. $k \cdot J = kJk^{-1}$
$|K| = 5$, so every orbit has size 1 or 5 by the Orbit-Stabilizer Theorem. In particular, the orbit of H $\mathcal{O}_H$ has size 1 or 5.

Case 1. $|\mathcal{O}_H| = 1$. I.e., $\forall k \in K : kHk^{-1} = \{khk^{-1} : h \in H\} = H$.
Now let $K \curvearrowright H$ by conjugation. $k \cdot h = khk^{-1}$. Orbits have size 1 or 5. But $|H| = 3$ So every orbit has size 1. I.e., $\forall k \in K, \forall h \in H : khk^{-1} = h$, so $kh = hk$. Hence (in this case), $G \cong H \times K$.

Case 2. $|\mathcal{O}_H| = 5$ I.e., there are 5 distinct subgroups of the form $kHk^{-1}, k \in K$. Then $G = \bigcup_{S \in \mathcal{O}_H} S \cup K$, as each pair of subgroups in $\mathcal{O}_H$ has intersection e_G. Also K exists, so the subgroups of G are either in $\mathcal{O}_H$ or equal to K. Thus, K is the *unique* subgroup of G of cardinality 5. In particular, $\forall g \in G : gKg^{-1}$ also has cardinality 5, so $gkg^{-1} = K$, hence $K \trianglelefteq G$. Let $H \curvearrowright K$ by conjugation. $h \cdot k = hkh^{-1} \in K$.

CLAIM (1). $\exists k_0 \in K$ such that $k_0 \neq e_G$ and $\forall h \in H : hk_0h^{-1} = k_0$

PROOF. Let p be the number of fixed points. By Fixed-Point Lemma,$p \equiv |K| \pmod 3$. However, $|K| \not\equiv 1 \pmod 3$, so $p \geq 2$. Thus, there exists a non-identity fixed point (k_0)[1]. □(Claim)

So, $\forall h \in H : hk_0 = k_0h$. Since $k_0 \neq e$, $|k_0| = 5$, hence $K = \langle k_0 \rangle$. Since $hk_0^n = k_0^n h$, and h was arbitrary, we know that $\forall h \in K, \forall k \in K : hk = kh$. Thus, $G \cong H \times K$. □(Thm).

PROPOSITION 88. *(p=2) Suppose $q > 2$ is prime. Then there exists (up to isomorphism) a* unique *non-cyclic group G with $|G| = 2q$.*

PROOF SKETCH. Fix (by Cauchy) $x, y \in G$ such that $|x| = 2$, $|y| = q$, then put $H = \langle x \rangle$ and $K = \langle y \rangle$.
We posit that $K \trianglelefteq G$ (verification left as an exercise).
So $H \curvearrowright K$ by conjugation. So, $xyx^{-1} \in K$ $\exists r : 0 < r < q$ such that $xyx^{-1} = y^r$, $xy^2x^{-1} = (xyx^{-1})(xyx^{-1}) = y^{2r}$. Thus, it is apparent that $xy^jx^{-1} = y^{jr \pmod q}$
But also,

$$y = x^2y^2x^{-2} = x(xyx^{-1})x^{-1} = x(y^r)x^{-1} = y^{r \cdot r}$$

So, $r^2 \equiv 1 \pmod q$
Exercise: The only solutions to $r^2 \equiv q \pmod{()q}$ are $r \equiv 1, -1 \pmod q$.

Case 1. $(r = 1)$: $xyx^{-1} = y$, i.e., $xy = yx$. Hence, $G \cong \langle x \rangle \times \langle y \rangle = H \times K$, cyclic.

[1]Note that this is where we needed the hypothesis that $q \not\equiv 1 \pmod p$.

Case 2. ($r = -1$): $xyx^{-1} = y^{-1}$. Shuffle to obtain $yx = xy^{-1}$.
We know that $G = \{x^i y^j : i \in \{0,1\}, j \in \{0,\dots,q-1\}\} = HK$.
To multiply, $(x^i y^j)(x^\ell y^k) = \begin{cases} (x^i y^{j+k}) & \text{if } \ell = 0 \\ x^i(y^j x)y^k = x^i x y^{-j} y^k = x^{i+1} y^{k-j} & \text{if } \ell = 1 \end{cases}$
Hence, the group operation is completely determined by $yx = xy^{-1}$, and so there is at most one non-cyclic group (up to isomorphism) of cardinality $(\mathbb{Z}/q\mathbb{Z})$.
To show the existance of such a group, given $n \geq 3$, we consider the dihedral group of cardinality $2n$, where the dihedral group is the group generated by reflection and rotation on the regular n-polygon. □

Lecture 19 (2016–02–29)

Definition 89. Let $H \leq G$ be groups. The normalizer of H in G is $N_G(H) = N(H) = \{g \in G : g^{-1}Hg = H\} = \{g \in G : gHg^{-1} = H\}$

Fact/Exercise:
(1) $N(H) \leq G$
(2) $H \trianglelefteq N(H)$

Theorem 90 (Sylow 1). *Suppose that G is a finite group, p is prime, and p^i divides $|G|$ for some $i \in \mathbb{Z}$. Then $\exists H \leq G$ such that $|H| = p^i$.*

Proof. Proceed by induction on i.
If $i = 0$ then trivial as $H = \{e\}$, the trivial subgroup. If $i = 1$ then this is true by Cauchy.
Our stategy is to suppose we have $H_i \leq G$ of cardinality $|H_i| = p^i$. and p^{i+1} divides $|G|$. We will find $H_{i+1} \supseteq H_i$ with $H_{i+1} \leq G$ and $|H_{i+1}| = p^{i+1}$.
Intuition: Consider the cosets of H_i in G. We're going to pick out p cosets of H_i $g_1 H g_2 H, \dots, g_p H$ such that $\bigcup_{i=1}^{p} g_i H$ is a subgroup of G.
Let $X = G/H_i = \{gH_i : g \in G\}$. Note that $|X| = \frac{|G|}{|H_i|} = \frac{p^z m}{p^i}$(where $z > i$) $\equiv 0 \pmod p$.
Let $H_i \curvearrowright X$ by left multiplication. $h \cdot (gH_i) = (hg)H_i$.

Claim (1). $gH_i \in X$ is a fixed point of the action iff $g \in N(H_i)$.

Proof. gH_i is a fixed point iff $\forall h \in H_i (h \cdot (gH_i) = gH_i)$ iff $(hg)H_i = gH_i$ iff $g^{-1}hg \in H_i$. Thus, $g^{-1}H_i g \in H_i$ so, as they are finite sets with the same cardinality and conjugation is an injective map, $g^{-1}H_i g = H_i$, meaning $g \in N(H_i)$ □(C1)

By Fixed-Point Lemma, since H_i is a p-group, we know that # fixed points $\equiv |X| \pmod p$. The number of cosets fixed by the action is a multiple of p. This is equivalent to saying p divides $|N(H_i)/H_i|$ (i.e., the number of cosets represented in the normalizer is a multiple of p). Since $H_i \trianglelefteq N(H_)i$, $N(H_i)/H_i$ is a quotient group. So by Cauchy, we may take $g \in N(H_i)$ such that $|gH_i| = p$ in $N(H_i)/H_i$.
Intuition: As we cycle through the powers of g, we get the cosets we're going to choose.
Finally, let $H_{i+1} = \bigcup_{k=0}^{p-1} g^k H_i = \{g^k h : h \in H, 0 \leq k < p\}$.
Note that $|H_{i+1}| = p^{i+1}$ as it's a union of p disjoint cosets of cardinality p^k.

Claim (2). H_{i+1} is a subgroup of G.

Proof.

- $e_G \in H_{i+1}$

- $h_1, h_2 \in H_{i+1} \implies h_1h_2 \in H_{i+1}$
  Fix k, ℓ such that $x, y \in H_i$ and $h_1 = g^k x, h_2 = g^\ell y$.
  Since $g \in N(H_i), \exists z \in H_i$ such that $g^{-\ell} x g^\ell = z$. So,
$$h_1h_2 = g^k x g^\ell y = g^{k+\ell} \underbrace{zy}_{\in H_i} \in H_{i+1}$$

$\square$(C2)

$\square$(Thm)

Definition 91. For p prime, $H \leq G$ (finite),is a Sylow p-subgroup if $|H|$ is the largest power of p dividing $|G|$. i.e., if, $|G| = p^k m, \gcd(p, m) = 1$. Then $|H| = p^k$.

Theorem 92 (Sylow 2). *Any two Sylow p-subgroups of G (finite) are conjugate.*

Proof will come later.

Theorem 93 (Sylow 3). *If $|G| = p^k m, \gcd(p, m) = 1$, then the number of Sylow p-subgroups n_p satisfies $n_p | m$ and $n_p \equiv 1 \pmod p$.*

Proof will come next lecture, first let's see an example.

Example.

a) Every group G with $|G| = 15 = 3 \cdot 5$ is cyclic.
   $n_3 | 5 \implies n_3 \in \{1, 5\}$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 1$. $n_5 = 1$. Thus, $\exists H, K \trianglelefteq G$ with $|H| = 3, |K| = 5$. So, by Corollary 84, $G \cong H \times K$.
b) There are (up to isomorphism) exactly two groups G with cardinality $99 = 3^2 \cdot 11$. Sylow 3-subgroup has cardinality 9. $n_3 = \#$ of subgroups of cardinality 9.
   $n_3 | 11 \implies n_3 \in \{1, 11\}$. As $n_3 \equiv 1 \pmod 3$, it can't be 11, so $n_3 = 1$
   $n_{11} = \#$ of subgroups of cardinality 11. $n_{11} | 9$ and $n_{11} \cong 1 \pmod 1 1$ means that $n_{11} = 1$.
   Fix unique $H, k \trianglelefteq G$ with $|H| = 9, |K| = 11, H \cap K = \{e\}$. So $G \cong H \times K$.
   Case 1: $H \cong \mathbb{Z}/9\mathbb{Z}$. Then $G \cong \mathbb{Z}_9 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{99}$.
   Case 2: $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ then $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_1 1 \cong \mathbb{Z}_3 \cong \mathbb{Z}_{33}$.

Lecture 20 (2016–03–02)

Proof of Sylow 2. Fix two Sylow p-subgroups $P, Q \leq G$ such that $|P| = |Q| = p^k$. Let $X = G/P$ and let $Q \curvearrowright X$ by left multiplication, i.e., $\forall h \in Q : h \cdot (gP) = (hg)P$.
Note that $|X| = \frac{p^k m}{p^k} = m \not\equiv 0 \pmod p$. Since Q is a p-group, by Fixed-Point Lemma, the number of fixed points is equivalent to $|X| \bmod p$, so we can choose a fixed point $gP \in X$. We know that for any $h \in Q, h \cdot (gP) = gP$, so $(hg)P = gP$, meaning $g^{-1}hg \in P$.
As $h \in Q$ was arbitrary, $g^{-1}Qg \subseteq P$. As $|g^{-1}Qg| = |P| = p^k$, it follows that $g^{-1}Qg = P$. $\square$

We prove both parts of Sylow 3 separately, as they are somewhat dissimilar

Proof of Sylow 3 (a). Let $X = \{H \leq G : |H| = p^k\}$ be the set of all Sylow p-subgroups of G. so $|X| = n_p$. Let $G \curvearrowright X$ by conjugation, i.e., $g \cdot H = gHg^{-1}$. For convenience, fix some designated Sylow p-subgroup $P \in X$ (which exists by Sylow 1).
This time we're going to use the Orbit-Stabilizer Theorem
By Sylow 2, we know that $\mathcal{O}_P = X$, so $|\mathcal{O}_P| = n_p$. By the Orbit-Stabilizer Theorem, we know that $|\mathcal{O}_P| \cdot |G_P| = |G|$, so $n_p = |G|/|G_p|$. Note also that $|G| = p^k m$.

Note that $P \leq G_P$ since $\forall g \in P, gPg^{-1} = P$. So, by Lagrange's Theorem, we know that $|P|$ divides $|G_P|$, so say $|G_p| = p^k\ell$. Thus, $n_p = \frac{p^k m}{p^k \ell} = \frac{m}{\ell}$. This shows that $m = n_p\ell$, meaning that n_p divides m as desired. $\square$

Proof of Sylow 3 (b). Again let $X = \{H \leq G : |H| = p^k\}$ be the set of all Sylow p-subgroups of G. so $|X| = n_p$. Fix $P \in X$ (which exists by Sylow 1). Let $P \curvearrowright X$ by conjugation.
We know that $P \in X$ is a fixed point of $P \curvearrowright X$.

Claim. P is the only fixed point.

Proof (Claim). Suppose $Q \in X$ is a fixed point. Want to show $Q = P$. So, $\forall g \in P$ $g^{-1}Qg = Q$, i.e., $P \leq N(Q)$. We also know that $Q \leq N(Q)$. So, P, Q are both Sylow p-subgroups of $N(Q)$. By Sylow 2, $\exists h \in N(G)$ st $Q = h^{-1}Qh = P$. Hence, $Q = P$. $\square$(Claim)

So the number of fixed points of $P \curvearrowright X$ is 1. P is a p-group, so by the Fixed-Point Lemma, we have $n_p = |X| \equiv 1 \pmod p$ $\square$(Sylow 3b)

Example. Let's classify all *abelian* groups G with cardinality 108 (up to isomorphism).
First we note that $108 = 2^2 \cdot 3^3$
By Sylow 1, there exist $H, K \leq G$ such that $|H| = 2^2$ and $|K| = 3^3$.
Since G is abelian, $H \trianglelefteq G$ and $K \trianglelefteq G$.
Also, $H \cap K = \{e\}$ by Lagrange's Theorem (since $\gcd(2^2, 3^3) = 1$). So by corollary 84, $G \cong H \times K$.
(We write $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$, although some number theorists would beg to differ.)
First H. H is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Next, K. $|K| = 27$ and it's abelian (because it's a subgroup of G.)
Case 1 ($\exists k \in K$ such that $|k| = 27$):
    In this case, $K \cong \mathbb{Z}_{27}$
Case 2 (No element of order 27, but $\exists k \in K$ such that $|k| = 9$):
    We posit that we may take $g \in K/\langle k\rangle$ with $|g| = 3$. (Existance left as an exercise to the reader).
    $\langle g\rangle \cap \langle k\rangle = \{e\}$. Thus, by corollary 84, $K \cong \mathbb{Z}_9 \times \mathbb{Z}_3$
Case 3 (All elements have order 3):
    Exercise: use Sylow's theorem to show $K \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_3$
These cases are exhaustive, so we have 6 options.
Thus, G could be isomorphic to the direct product of any tuple in $\{\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2\} \times \{\mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3\}$

Cool note: we won't get to this, but every finite abelian group is isomorphic to the direct product of a direct product of cyclic groups.

Index